UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,417	11/06/2000	Vance C. Bjorn	003022.P019X	9958

7590 04/21/2005

Judith A. Szepesi
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/707,417	BJORN, VANCE C.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the appeal brief filed on 24 January 2005.

2. Claims 1-31 are pending in the application.

3. Claims 1-31 have been rejected.

Response to Arguments

4. In view of the appeal brief filed on 24 January 2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1, 5, 6, 8, 9, 11-14, 17, 23, 24, 26, 27 and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Dickinson et al U.S. Patent No. 6,853,988 B1.

As to claims 1, 14 and 17, Dickinson et al discloses a method of authenticating a client, the method comprising:

receiving a record ID for a user [column 7, lines 8-30], and a one-time key generated by the server and encrypted with a user's public key by the server [column 28 line 66 to column 29 line 27];

receiving the user's authentication data from the client [column 29, lines 28-38];

determining if the user's authentication data matches the record ID [column 29, lines 28-38]; and

if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client [column 29, lines 39-51].

As to claims 5 and 23, Dickinson et al discloses a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server [column 14, lines 16-21].

As to claims 6 and 24, Dickinson et al discloses that the client's authentication data is automatically redirected to the authentication server [column 14, lines 34-57].

As to claims 8 and 26, Dickinson et al discloses that the authentication data is personal data selected from among the following: a password, a smart card; and another type of authentication card [column 12, lines 21-32].

As to claims 9 and 27, Dickinson et al discloses that the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key [column 7, lines 53-65].

As to claims 11 and 29, Dickinson et al discloses that the record ID and the encrypted one-tune key are further encrypted using a partner key. Dickinson et al discloses decrypting the record ID and encrypted one-time key using the partner key [column 48 line 62 to column 49 line 13].

As to claims 12 and 30, Dickinson et al discloses that the partner key is a symmetric key set up during registration of the partner [column 8, lines 7-14].

As to claims 13 and 31, Dickinson et al discloses that the partner key is a private key of the authentication server [column 8, lines 7-14].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-4 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 as applied to claim 1 above, and further in view of Smith et al U.S. Patent No. 6,233,685 B1.

As to claims 2 and 20, Dickinson et al teaches receiving a registration authentication data from the user, as discussed above.

Dickinson et al does not teach generating a random public key/private key pair for the user. Dickinson et al does not teach generating a random record ID for the user. Dickinson et al does not teach associating the authentication data and the private key with the record ID.

Smith et al teaches generating a random public key/private key pair for the user [column 5, lines 34-46]. Smith et al teaches generating a random record ID for the user. Smith et al teaches associating the authentication data and the private key with the record ID [column 8 line 66 to column 9 line 19].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that the user's public/private key pair would have been generated randomly by the server. The server would have generated a

record ID for the user randomly. The authentication data and the private key would have been associated with the record ID.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Smith et al because it minimizes risk of compromised factory machines, activating tamper response at a point of trust (certifying authority) to protect against attacks, and/or continually certifying the untampered state of the device along shipping channels and at user sites, and/or allowing for all keys to be regenerated so that in accordance with sound cryptographic practice there is no need to depend on permanent keys [column 2, lines 45-56].

As to claims 3 and 21, Dickinson et al teaches sending the record ID and the public key to the user [column 11, lines 28-35].

As to claims 4 and 22, Dickinson et al teaches establishing a secure connection with the user, prior to receiving registration authentication data [column 6, lines 13-29].

7. Claims 7, 10, 25 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 as applied to claim 1 above, and further in view of Byford U.S. Patent No. 6,581,161 B1.

As to claims 7, 10, 25 and 18, Dickinson et al teaches that the authentication data is biometric data [figure 1].

Dickinson et al does not teach discarding the record ID after returning the one-time key to the user.

Byford teaches authentication data being biometric data [column 4 lines 44-58]. Byford teaches discarding a user's record ID [column 2, lines 39-42].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that the authentication data was biometric data and the user's record ID would have been discarded.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Byford because it removes the need for encoded badges, static passwords and the like, and also removes the need for users to present themselves at a particular location, such as a security control office, before they can be granted access rights to a facility [column 4, lines 59-67].

8. Claims 15, 16, 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 as applied to claims 14 and 17 above, and further in view of Towers et al U.S. Patent No. 5,692,106.

As to claims 15, 16 and 18, Dickinson et al does not teach determining an authentication policy associated with the user. Dickinson et al does not teach verifying that the authentication policy has been satisfied, prior to permitting access to the server. Dickinson et al does not teach determining if the server should verify additional data. Dickinson et al does not teach requesting additional data from the user prior to generating the onetime key.

Towers et al teaches determining an authentication policy associated with the user [column 13, lines 31-48]. Towers et al teaches verifying that the authentication policy has been satisfied, prior to permitting access to the server [column 13, lines 31-48]. Towers et al teaches determining if the server should verify additional data [column 1, lines 36-63]. Towers et al teaches requesting additional data from the user prior to generating the one-time key [column 1, lines 36-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that an authentication policy associated with the user was verified prior to permitting access to the server. Should additional user information was needed; it would have been requested prior to generating the one-time key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Towers et al because the examiner asserts that authentication policies restrict what a user can do on a server site and requesting additional data further authenticates a user prior to accessing a server's site.

As to claim 21, Dickinson et al teaches that the interface sends the record ID and the public key to the user, as discussed above.

9. Claims 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dickinson et al U.S. Patent No. 6,853,988 B1 as applied to claim 17 above, and further in view of Mao U.S. Patent No. 6,119,227.

As to claim 19, Dickinson et al does not teach nonce generation logic to generate a nonce. Dickinson et al does not teach that the nonce is to be included with the user authentication data from the client. Dickinson et al does not teach comparison logic to verify that the user authentication data includes the appropriate nonce.

Mao teaches nonce generation logic to generate a nonce [column 5, lines 13-29]. Mao teaches that that the nonce is to be included with the user authentication data from the client [column 5, lines 30-51]. Mao teaches comparison logic to verify that the user authentication data includes the appropriate nonce [column 5, lines 30-51].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al so that there was nonce generation logic to generate a nonce. The nonce is would have been included with the user authentication data from the client. Comparison logic would have been used to verify that the user authentication data includes the appropriate nonce.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dickinson et al by the teaching of Mao because it provides a method for authenticating a user's requests and messages [column 1, lines 49-67]

As to claim 22, Dickinson et al teaches that interface establish a secure connection with the user, prior to receiving registration authentication data, as discussed above.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
April 14, 2005

AU 2131
4/17/05